REMARKS/ARGUMENTS

Reconsideration is respectfully requested.

Claims 1-12 are pending before this amendment. By the present amendment, claims 1, 3, 5, 9, and 11 are amended. No new matter has been added.

In the office action (pages 2-3), the specification stands objected to because of informalities. The applicants have amended the disclosure to address the informalities as suggested by the examiner. Therefore, the applicants respectfully request withdrawal of the above objections for paragraphs [19] and [76].

In the office action (page 3), claims 1, 3, and 5 stand objected to because of informalities. Claims 1, 3, and 5 have been amended as suggested by the examiner (i.e.; delete lease and insert **least**). The applicants respectfully submit that claims 1, 3, and 5 are now in compliance. Therefore, withdrawal of the aforementioned objection is respectfully requested.

In the office action (page 3), claims 1, 3 and 5 stand objected under 35 U.S.C. §112, ¶2, as being indefinite. In response, the applicants have amended the claims to address these rejections. More specifically, the amended claims 1, 3, and 5 now recite inter alia: --~~M/n-bit~~ M/m-bit intermediate data--. Therefore, the applicants respectfully requested withdrawal of the §112, ¶2 objection.

In the office action (page 4), claims 1-12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Publication No. 2002/0131588 (Yang) in view of U.S. Patent No. 6,230,257 (Roussel). The "et al." suffix is omitted in a reference name.

The applicants respectfully disagree.

The present invention relates to a rijndael block cipher apparatus including an operational unit for efficiently performing a round operation for encrypting/decrypting the rijndael block cipher, where the rijndael block cipher apparatus is made to mount in a mobile terminal such as a cellar phone and a PDA or a smart card, which requires a high-rate and small-sized cipher processor, and which can encrypt and decrypt important data that requires security at high speed (specification page 2 [11] and [12]). The rijndael block cipher apparatus uses the rijndael algorithm that require a number or round where the number of rounds performed for the rijndael block cipher apparatus is determined by the number of bits used by the round keys (specification page 1 [7]).

The rijndael algorithm of the present invention supports a variable block length of an SPN (Substitution-Permutation Network) structure, and enables the use of 128-bit, 192-bit, and 256-bit keys with respect to the respective block lengths (specification page 1 [7]).

The key lengths determine the number of rounds in the rijndael algorithm, where the 128-bit keys recommend using 10 rounds and the192-bit and 256-bit keys use 12 and 14 rounds respectively. For example, the present invention discloses a rijndael algorithm using a 128-bit key that reduces hardware implementation of the rijndael algorithm over the prior art. Typically, the rijndael algorithm encrypts/decrypts data for the rijndael block encryption/decryption by repeating round operations where a round operation for the encryption process of the rijndael block cipher is composed of four transforms of substitution, shift_row, mixcolumn and add-round-key, and a round operation for the decryption process is composed of four transforms of inverse-shift_row, inverse substitution, add-round-key and inverse mixcolumn. As a result, the times

required for the round operation for the rijndael block cipher and hardware resources is vital to the performance of a rijndael cipher processor for cellar phone and a PDA or a smart card, which requires a high-rate and small-sized cipher processor (specification pages 1 and 2 [9] [10]).

The present invention reduces the hardware by transforming the 128-bit input key into a 128-bit round key for encryption/decryption by dividing the 128-bit input data into upper 64 bits and lower 64 bits and **simultaneously** performing the round operations for each the upper and lower 64 bits of input data. For example, the upper 64-bit data is added with the upper 64-bit round key generated by the round key generation unit while **simultaneously performing a mixcolumn of the lower 64-bit data.**

That is, the rijndael algorithm of the present invention discloses encrypting/decrypting the divided data (i.e.; upper and lower 64-bit data) for the rijndael block encryption/decryption by repeating round operations where a round operation for the encryption process of the rijndael block cipher is composed of four transforms of substitution, shift_row, mixcolumn and add-round-key, and a round operation for the decryption process is composed of four transforms of inverse-shift_row, inverse substitution, add-round-key and inverse mixcolumn where different transforms of the divided data are **simultaneously** performed on the upper and lower input data bits at the same time before the end of each round to generate the encrypted/decrypted data of 128, 192, or 256 bits respectively to/from a cellar phone and a PDA or a smart card that require high-rate and small-sized cipher processor (specification page 8 [18]).

Claim 1 has been amended to clarify this aspect of the present invention. Claim

1 now recites, inter alia:

> --**wherein the round keys generated in the add-round-key generation unit is added to a first M/m input data simultaneously during the processing of a second M/m input data of the round execution unit before the end stage of every round**--.

Nowhere does Yang and/or Roussel, alone or in combination, teach or suggest amended claim 1 of the present invention,and one skilled in the art would not have been motivated at the time the invention was made to modify the cited references to produce the claimed invention.

In contrast, Yang relates to providing the proper key for a block size of data for each round and outputs the respective key to the block round unit 203. Yang discloses that Round _Key [127:0] is only inputted to the Key mixer 404 only **after** the data has been inputted to the shifter 402 and then to the mixer 403. That is, "the inputted block data passes through the data conversion unit 401, shifter 402, mixer 403, and key mixer 404 **sequentially** so as to complete one round" (Yang [0052] and FIG. 4). Further, Yang teaches away from dividing up the input data, where Yang discloses finding the key for encryption or decryption of one block every round so as to **output** the found key to the block round unit 203. Hence, the register having the **key value only** required for a round is necessary (Yang [0045]). For example, if the block size is 128 bits and a size of the key value is 256 bits, the register **needs** a value of (block size*value for one round), the required size of the register is 128*1=16 bytes (Yang [0046]), and **not** a key value of 64-bits as disclosed by the present invention.

Further, Yang teaches "the block round unit **completes** all round calculation of data having been currently encrypted or decrypted **before a next block data is**

inputted from the control unit and then stores the corresponding result in the output buffer of the control unit" (Yang [0015]). Because Yang discloses that the register having the "**key value only required for a round is necessary**" (Yang [0045]), Yang's needs the actual key value (i.e.; not a partial value) for the start of each round where the key values must be 128, 192 or 256 (i.e.; the AES encryption/decryption key values).

Therefore, because Yang discloses that an input block of data performs the transforms (i.e.; conversion, mixer, and key mixer) for each round sequentially and completes all round calculations before the next block on data is inputted with block size key values 128, 196, or 256, Yang teaches away from performing the transform of the key mixer (Add_Round_Key) on a first input data while simultaneously performing the transform of the mixer on a second input data, where the first and second input data is half the key value of inputted data (Yang [0037] and table 1).

Thus, because Yang **requires** the key value (i.e.; 128, 192, or 256) used in rijndael block cipher algorithm, one skilled in the art would not have been motivated to use the staggering execution of a single packed date instruction using the same circuit from Roussel where the key values would less that 128, 192, or 256 respectively. Also, because Yang completes all rounds that require the actual key values (i.e.; not a partial key value) before receiving data to start another round, Yang teaches away from performing different transforms on the two different inputted data having partial key values before the end of each round at the same time.

In contradistinction, the present invention discloses performing the transform of add round key to the upper 64-bit while simultaneously performing the transformation of a mixcolumn on the lower 64-bit data during the same clock cycle. That is, the rijndael

block cipher apparatus of the present invention performs all round operations for encrypting and decrypting input data for rijndael block encryption/decryption in the unit of 64 bits (upper and lower 64-bit data), and to generate round keys required for the round operations of the upper 64-bit data "**simultaneously**" with performing the transformation of mixcolumn of the round operations for lower 64-bit data (specification [33], [89], [102], [110], [111], and [116].

In contrast Yang **only sequentially performs** the round operation transformations of conversion, shifter, mixer, a key mixer on the first inputted data that requires the key values (i.e.; not partial values) required for the rijndael algorithm before performing **any** transforms of the round operation on a second inputted data (Yang [0015] and [0045]).

Accordingly, neither Yang nor Roussel, whether considered alone or in combination, teaches nor suggests amended claim 1 of the present invention, which recites, inter alia: --wherein the round keys generated in the add-round-key generation unit is added to a first M/m input data simultaneously during the processing of a second M/m input data of the round execution unit before the end stage of every round--. Also, one skilled in the art would not have been motivated at the time the invention was made to modify the cited references to produce the claimed invention.

Therefore, an indication of allowable subject matter with respect to claim 1 is respectfully requested.

As to claim 2, the applicants respectfully submit that claim 2 is allowable at least since it depends from claim 1, which is now considered to be in condition for allowance

Independent amended claims 3, 5, 9, and 11 recite similar features to those found in claim 1. Therefore, for reasons analogous to those argued above with respect to claim 1, amended claims 3, 5, 9, and 11 are patentable over the applied references.

As to claims 4, 6-8, 10 and 12, the applicants respectfully submit that these claims are allowable at least since they depend from either claim 3, 5, 9 or 11, which are now considered to be in condition for allowance for the reasons mentioned above for claim 1.

For the reasons set forth above, the applicants respectfully submit that claims 1-12, now pending in this application, are in condition for allowance over the cited references. Accordingly, the applicants respectfully request reconsideration and withdrawal of the outstanding rejections and earnestly solicit an indication of allowable subject matter.

This amendment is considered to be responsive to all points raised in the office action. Should the examiner have any remaining questions or concerns, the examiner is encouraged to contact the undersigned attorney by telephone to expeditiously resolve such concerns.

Respectfully submitted,

Dated: 10/23/2008

Keith S. Van Duyne

Keith S. Van Duyne, Reg. No. 54,505
Ladas & Parry LLP
224 South Michigan Avenue
Chicago, Illinois 60604
(312) 427-1300